第5回情報セキュリティ・シンポジウムの模様

―デジタル署名の長期的な利用とその安全性―

1．はじめに

日本銀行金融研究所は、2003年3月7日、「デジタル署名の長期的な利用とその安全性」をテーマとして、第5回情報セキュリティ・シンポジウムを開催した。

今回のシンポジウムの問題意識は、電子商取引や電子政府等の分野で電子文書の作成者や完全性を確認する手段としてデジタル署名の利用が拡大しつつあることを踏まえ、今後、デジタル署名について、紙の文書における署名・捺印と同等の効果を期待して利用していくことを想定すると、デジタル署名の長期的利用に伴う問題点や、これを解決するための方策を検討しておく必要があるのではないかというものである。

今回のシンポジウムは、キーノート・スピーチ、研究発表、パネル・ディスカッションの順に進められた後、東京大学・今井秀樹教授による総括コメントによって締め括られた（プログラムは、下表のとおり）。また、フロアには、情報技術に関連する学界、行政、金融機関、電機メーカー等から、研究者・実務家約90名の参加を得た。

〈プログラム〉

キーノート・スピーチ「デジタル署名の長期的な利用とその安全性について」 ：松本勉（横浜国立大学教授）
研究発表「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」 ：宇根正志（日本銀行金融研究所研究第2課）
パネル・ディスカッション「デジタル署名を長期的に安全に利用するために」
・パネル発表1：佐々木良一（東京電機大学教授）
・パネル発表2：松浦幹太（東京大学助教授）
・自由討議 パネリスト：松本勉、佐々木良一、松浦幹太 司会：岩下直行（日本銀行金融研究所研究第2課企画役）
総括コメント：今井秀樹（東京大学教授）

以下では、プログラムに沿って、キーノート・スピーチ、研究発表、パネル・ディスカッション、総括コメントの概要を紹介する（文責、日本銀行金融研究所。文中敬称略）。

2．キーノート・スピーチ「デジタル署名の長期的な利用とその安全性について」

松本は、岩下との共同論文[1]に基づき、デジタル署名付き電子文書の長期的な利用の現状、および、問題点と対策の方向性について以下のとおり発表した。

(1) デジタル署名付き電子文書の長期的な利用

インターネットの急速な発達と高性能なパーソナル・コンピュータの普及に伴い、さまざまな産業分野において、デジタル化された文書（電子文書）の利用が拡大している。2001年4月には「電子署名及び認証業務に関する法律」（電子署名法）が施行され、一定の基準を満たすデジタル署名が本人により付与された電子文書について、本人の署名・捺印の付された紙の文書と同等に「その文書が真正に成立したものと推定する」という効力が認められた。デジタル署名を利用することによって、電子文書の偽造や改ざんなどの脅威に対処しつつ、さまざまな取引の電子化を進めていくための基盤が整備されたといえる。

しかし、現時点では、電子文書にデジタル署名を付与して真正な成立の推定の効果を得ようとするシステムは少ない。オープン・ネットワークからのシステムへのアクセスにおける本人確認と電子文書の完全性確認の手段としてデジタル署名が利用されるケースがほとんどであり、デジタル署名は「取引の瞬間」に利用されるにとどまっているのが実情である。

(2) デジタル署名を長期間利用する際の問題と対応策

電子文書の完全性を長期間確保する手段としてデジタル署名が採用されていないのは、通常のデジタル署名だけでは、電子文書の完全性確保等の効力を長期間維持することが困難であるためと考えられる。これは、①時間の経過とともに、コンピュータのコスト・パフォーマンスや暗号解読技術の向上等によってデジタル署名の安全性が低下する、②同一の管理方法を前提とすれば、署名生成用の秘密鍵が漏洩する危険性が時間の経過とともに高くなる、③公開鍵証明書の有効期間が切れると、

1 松本勉・岩下直行、「デジタル署名の長期的な利用とその安全性について」（『金融研究』第22巻別冊第1号、日本銀行金融研究所、2003年6月）を参照。

署名生成用の秘密鍵が安全に管理されているか否かを確認不可能になる等の理由によるものである。長期保管のために特別な対策が講じられていない通常のデジタル署名方式の場合、その効力が維持され、内容を信頼することができる期間は、たかだか公開鍵証明書の有効期間内（実際には1年程度）と考えるべきである。

署名・捺印のある紙の文書にも、ごく短期的にしか利用しないものと、長期間の保管を前提とするものがあるように、電子文書も、使用される状況によって長期保管の必要性が異なってくる。従来は、取引の過程で一時的に利用され、長期的に保持される必要のない書面が電子化されていたため、電子文書を長期保管するニーズはあまりなかった。しかし、紙の文書から電子文書への移行が確実に進んでおり、法律によって交付が義務付けられる書面や、行政手続に用いられる書面までもが電子化されつつあるため、デジタル署名の安全性を長期間確保する方法を検討する必要性が高まっている。具体的には、次のような対応策が考えられる。

対応策1：デジタル署名を検証したうえで保管し、ログなどの保管記録を取得しておき、後日署名が偽造された疑いが発生した場合、保管記録に基づいて判断する。
対応策2：デジタル署名付き電子文書を受信した時点で外部機関からデジタル・タイムスタンプを発行してもらい、署名付き電子文書を特定の日時に受信したことの証明を取得しておく。
対応策3：デジタル署名に対応する公開鍵証明書の有効期間が切れる前に、署名付き電子文書の更新を行う。
対応策4：通常のデジタル署名ではなく、署名生成機能の危殆化[2]対策が講じられた署名方式を利用して署名付き電子文書を生成してもらう。

(3) 電子政府における電子文書の長期的利用

現在構築が進められている電子政府の電子申請・届出システム等では、旧総務庁・行政管理局が開催した共通課題研究会で検討された「電子文書の原本性確保」の考え方に基づき、原本性を確保するための装置（原本性保証装置）に電子文書を格納して長期保管するという仕組みが採用されている。原本性保証装置は、ID・パスワード等によってアクセス制御されるハードウエアであり、電子文書の更新履歴を確実に記録する機能を備えている。こうした方法は、上記の「対応策1」をシステム的に実現したものといえる。

しかし、「対応策1」に頼ったシステムにおいては、万一防御機構が破られ、一部の電子文書についてセキュリティが損なわれると、当該システムに格納されている

2 署名生成機能の危殆化とは、デジタル署名を生成するための秘密鍵が漏洩したり、ハードウエアが盗用されたりして、本来、秘密鍵の正当な所有者のみが利用できるはずの署名生成機能が、それ以外の者によっても利用できるようになることを意味する。

電子文書すべてが信頼を失うリスクがある。また、電子文書を長期間安全に保管できるのは原本性保証装置を利用している政府の側に限定され、国民が原本性保証装置を利用せずに保管した電子文書の安全性は長期的に保証されにくいという問題もある。このため、電子文書が保管されているシステム全体を防御するという現在の対応に加えて、デジタル署名が付与された電子文書単体に対する長期的な安全性を向上させるための対策を講じていくことが望ましいと考えられる。

(4) 今後の課題

今後、紙の文書から電子文書への移行がいっそう進んでいくことを考えると、デジタル署名方式を長期的に安全に利用できるようにするために、署名生成機能の危殆化対策が講じられたデジタル署名方式や、デジタル・タイムスタンプなどの新しい技術の採用について、積極的に検討していくことが重要と考えられる。

従来の紙の文書に基づくさまざまな商取引、行政手続の安定性、安全性は、署名･捺印そのものによって支えられてきたわけではない。署名・捺印のある紙の文書が、極めて精巧に偽造や変造ができたとしても、長年の経験により確立され、法律などの制度によっても支えられた「実務の枠組み」によって、取引の安定性が維持されていると考えるべきである。電子商取引や電子政府における情報セキュリティの問題点とは、こうした「実務の枠組み」を崩すことに伴う不安や取引の不安定化を、技術だけでは支えきれないことにあるといえる。電子文書を介して行われる取引については､現段階ではそうした実務の枠組みが確立していないのが実情である。電子文書の利用範囲を拡大し、そのメリットを最大限に活かしていくためにも、デジタル署名の長期的安全性について、今後検討を深めていくことが必要であろう。

3．研究発表「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」

宇根は、標題の研究論文[3]に基づき、署名生成用秘密鍵の漏洩とその対策技術に関して以下のとおり発表を行った。

(1) 署名生成用秘密鍵の管理と漏洩の影響

電子文書の完全性を確保するためにデジタル署名を利用する場合、署名生成用の秘密鍵が外部に漏洩することのないよう、厳格に管理する必要がある。認証機関が作成する認証ポリシーや認証実施規程では、公開鍵証明書の利用者の責任として

3 宇根正志、「デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策」(『金融研究』第22巻別冊第1号、日本銀行金融研究所、2003年6月）を参照。

「秘密鍵が第三者に漏洩しないように適切に管理すること」と規定されることが一般的である。現在でも、特に高度なセキュリティが要請される業務の場合、署名生成用の秘密鍵を、内部のデータを物理的・論理的に保護する機構を持つIC カード等のハードウエアに格納することが多い。しかし、いかなる形態で秘密鍵を管理するとしても、秘密鍵が何らかの要因で外部に漏洩する可能性を否定することはできない。万一、秘密鍵が漏洩した場合、漏洩した秘密鍵によって過去に生成された署名がすべて信頼できなくなり、デジタル署名の付与された電子文書の証拠としての機能が大きく損なわれることになるほか、社会的なインフラとしてのデジタル署名技術そのものに対する信頼も損なわれるおそれがある。電子文書の長期保管を考える場合、こうした秘密鍵漏洩への対策が重要なポイントとなる。

(2) 秘密鍵の漏洩形態

秘密鍵が漏洩する形態として、①鍵管理方法やその運用形態の欠陥による漏洩、②ハードウエアの解析による漏洩、③署名方式自体の安全性低下による漏洩の3つが想定される。

鍵管理方法等の欠陥が秘密鍵の漏洩につながることを示す事例として、暗号モジュールIBM4758の暗号処理ソフトウエアCCAの鍵管理方法を利用した攻撃方法に関する研究が挙げられる。本研究は、米国政府標準FIPS140-2に基づく認定を獲得した暗号モジュールIBM4758について、内部に格納された2-keyトリプルDESの鍵を効率的に推定可能なことを指摘したものであり、安全性について公的なお墨付きを得たハードウエアを利用していても、鍵管理方法次第で秘密鍵が漏洩するおそれがあることを示唆している。

また、ハードウエアが物理的に解析されて秘密鍵が漏洩するリスクも無視することはできない。ハードウエアの解析による漏洩を防ぐためには、セキュリティ要件に合致した安全性を有するハードウエアを採用する必要があるが、個々のハードウエアの安全性評価について学会等で議論されることは稀であり、利用者が各ハードウエアの安全性を適切に評価することも難しいからである。

署名方式等の欠陥による漏洩についても、実際にデジタル署名を利用したシステムにおいて安全性上の問題点が指摘されたいくつかの事例が存在しており、その可能性を考慮しておく必要がある。

(3) 秘密鍵の漏洩を前提とした対策

漏洩した秘密鍵による署名偽造への対策技術は、「秘密鍵を頻繁に更新することで秘密鍵漏洩によって信頼できなくなる署名を制限する技術」と「署名方式以外の仕掛けを利用して署名の偽造を検知する技術」に分けられる。

秘密鍵を頻繁に更新するというアイデアに基づく技術として、フォワード・セキュア（forward-secure）署名とキー・インシュレイティッド（key-insulated）署名が提

案されている。フォワード・セキュア署名は、一方向性関数を用いて秘密鍵を更新することで、漏洩した秘密鍵からそれよりも古い秘密鍵を導出困難にする。キー・インシュレイティッド署名では、別途安全に管理されるマスター鍵を用いて秘密鍵を更新することによって、漏洩した秘密鍵から他の秘密鍵を導出困難にする。

署名方式以外の仕掛けを利用して署名の偽造を検知する技術として、ヒステリシス（hysteresis）署名、実行ハードウエア確認タグ付き署名、MAC（message authentication code）付き署名が挙げられる。ヒステリシス署名とは、デジタル署名の生成履歴を安全な形で保管し、署名偽造の疑いが生じた場合、その署名と履歴データの整合性を確認することで、署名偽造の検知を可能にする技術である。同署名では、署名生成の都度、過去の署名履歴データを署名に埋め込むことにより、すべての署名が相互に関連付けられる。実行ハードウエア確認タグ付き署名は、複製困難な「耐クローン・モジュール」を署名生成用のハードウエアに格納し、耐クローン・モジュールの出力と署名付きデータから生成される「タグ」を用いて、署名が特定のハードウエアで生成されたか否かを確認可能にする技術である。MAC付き署名は、署名の生成にあわせてMACを生成して署名とともに保管し、署名偽造の疑いが生じた場合にはMACの検証によって偽造を検知する技術である。MAC生成用の秘密鍵は、署名生成用の秘密鍵とは別に、不正な書込みが困難な特殊なハードウエアに格納されることが想定されている。

(4) 秘密鍵漏洩対策技術の比較

想定される秘密鍵の漏洩形態については、フォワード・セキュア署名とキー・インシュレイティッド署名では、ハードウエアの解析による漏洩のみが想定されている一方、ヒステリシス署名、実行ハードウエア確認タグ付き署名、MAC署名では、上記(2)で述べた3種類の漏洩形態すべてが想定されている。セキュリティ要件の観点からみると、フォワード・セキュア署名とキー・インシュレイティッド署名では、どの秘密鍵が漏洩したのかを特定可能であることが必要となる一方、その他の技術では、信頼できる第三者が必要となるか、あるいは耐クローン・モジュール等の物理的な仮定が満たされる必要がある。

これらの技術の利用を検討する際には、今後のセキュリティ評価などの研究動向に注目するとともに、各技術によって想定環境やセキュリティ要件がそれぞれ異なっているため、個別のアプリケーションの想定環境やセキュリティ要件を十分考慮する必要がある。

4．パネル・ディスカッション
「デジタル署名を長期的に安全に利用するために」

(1) パネル発表1「デジタル署名の長期的安全性に関する検討」

佐々木は、デジタル署名の長期的な安全性を巡る議論のうち、特に、公開鍵暗号の危殆化を巡る問題とその対応策に焦点を当てて、以下のとおり説明した。

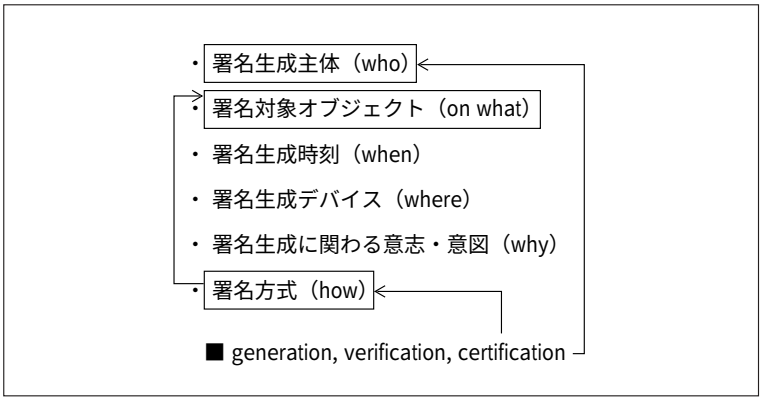
デジタル署名の長期的な利用において、署名生成用の秘密鍵が漏洩する原因を分類すると、①公開鍵暗号の危殆化、②ハードウエアの脆弱性、③署名プロトコルや実装方法の欠陥、④鍵管理方法の欠陥、⑤利用者の不注意の5種類に分けることができる。このうち、⑤の「利用者の不注意」による秘密鍵漏洩については、公開鍵証明書の失効と失効情報の配布を中心とした対応が考えられているが、それ以外の原因による秘密鍵漏洩に対しては、その対策が十分には検討されていないのが実情である。

特に、①の「公開鍵暗号の危殆化」は、デジタル署名に利用される公開鍵暗号技術そのものが安全ではなくなり、その暗号を利用しているすべての利用者の秘密鍵が漏洩リスクにさらされるという状況であり、その影響範囲が極めて広いため、あらかじめ十分な検討が行われていることが必要である。公開鍵暗号が危殆化するパターンは、(a)計算機のコスト・パフォーマンスの向上等による「漸進的な危殆化」、(b)特定の公開鍵暗号への新しい攻撃法の発見等による「飛躍的な危殆化」、(c)量子コンピュータなどの新しい計算機の出現や安全性のベースとなる数学の問題の効率的な解法の発見による「破局的な危殆化」の3つに分類することができる。いずれのパターンについても、危殆化した暗号方式の代替暗号が用意されていることが重要であるが、万一、(c)の「破局的な危殆化」が現実のものとなった場合、素因数分解問題や離散対数問題に依拠する暗号技術がすべて危殆化し、代替暗号すら存在しなくなるという状況も想定する必要がある。このため、既存の署名方式が依拠している数学問題とは別の問題（例えばナップザック問題）をベースとする署名方式や、計算量的にではなく情報量的に安全な署名方式等を代替方式として準備しておくことが望まれている。また、弱くなった署名方式を別の署名方式に迅速に切り替える方法に関しても検討しておく必要がある。

(2) パネル発表2「署名用秘密鍵漏洩後の紛争解決と5W1H」

松浦は、デジタル署名において確認の対象となる要素を整理することにより、秘密鍵漏洩時にも紛争解決が容易なシステムをどう設計するかという視点から、以下のとおり説明した。

図1　デジタル署名において確認の対象となる5W1H



デジタル署名は、「電子文書と、それを確認する署名生成者とを紐付ける」という特性を持つが、電子文書を長期間利用した際に、署名生成者の秘密鍵が漏洩すると、この署名生成者と電子文書とのリンクが破断してしまう。デジタル署名を巡る紛争解決を容易にするために、万一そのような事態に陥った場合でも、別の手段によってリンクを修復できるような設計としておくことが望ましい。そのようなシステムを検討するための視点として、デジタル署名で確認の対象となる要素を、図1のように「5W1H」に整理してみた。

この場合、通常のデジタル署名は、認証機関による公開鍵証明書の発行（certification）および特定の署名生成鍵と署名方式の利用（how）というルートを経由して、署名生成主体（who）と、署名対象オブジェクト（on what）を結び付ける仕組みと整理できる（図中の矢印を参照）。デジタル署名の生成において確認の対象となりうるのは、それ以外に、署名生成時刻（when）、署名生成デバイス（where）、署名生成にかかわる意志・意図（why）等が挙げられる。例えば、デジタル・タイムスタンプは“ when ”と“ how ”を結び付ける仕組み、署名を生成する際に能動的に実行しなければならない処理を組み込んだインターフェース等は“ why ”と“ how ”を結び付ける仕組みであり、これらによって通常のデジタル署名によるリンクを補強する役割を果たしている。

このように整理した場合、秘密鍵の漏洩は、“ who ”と“ on what ”のリンクを破断する事象と位置付けられる。こうした事象への対策としては、①5W1Hを含む関連情報を、取引ログとしてすべて安全にシステムに保管しておくという方法と、②“ who ”と“ on what ”を結び付ける別のルートを何らかの手段によって確保しておくという方法が考えられる。①のような「力業」も、適用システムによっては現実的な解となるが、今後の社会的なインフラ整備を想定した場合、②の方法についても検討していくことが必要となる。②を実現した事例としては、バイオメトリック認証によって“ who ”と“ where ”を結び付け、「MAC付き署名」と呼ばれる特殊なデジタル署名を利用して“ where ”と“ on what ”を結び付けることで、「別ルート」を構築してデジタル署名の証拠性を高める技術が研究されている。

この秘密鍵漏洩問題に代表されるように、PKIが整備された後も、デジタル署名を巡っては研究課題が山積している。それらの問題を解決するための技術的な研究に加え、新しい技術を活用するためにどのような運用モデルが必要になるかといった観点からも検討を進める必要がある。さらに、より長期的な視野に立って、「情報理論的に安全な署名方式」や「量子物理学を応用した署名方式」などに関する研究を推進していく必要があると考えられる。

(3) 自由討議、質疑応答

上記のキーノート・スピーチ、研究発表およびパネル発表の内容を受けて、パネリストによる自由討議およびフロアとの間での質疑応答が行われた。

まず、岩下は、本シンポジウムのテーマであるデジタル署名の長期的な安全性が、どの程度切実な問題と考えられるかについて、パネリストの見解を尋ねた。松本は、通常のデジタル署名が、秘密鍵の漏洩や公開鍵証明書の有効期限等の問題から長期的な利用に耐えられない構造を有していることを指摘したうえで、秘密鍵漏洩時の対策技術を検討しておくことが是非必要であり、問題は切実なものであると述べた。また、佐々木は、実際にデジタル署名付き電子文書を長期間利用する具体的なアプリケーションが多数想定されていることを指摘したうえで、こうした署名付き電子文書については、適切な有効期間を定めるとともに、有効期間が切れる前に更新・再交付を行う仕組みを構築していくことが今後是非必要となるとの見方を示した。

こうした意見を受けて、岩下は、通常のデジタル署名だけを電子文書に付加して長期保管するケースであっても、公開鍵証明書の有効期間等の問題はあるものの、デジタル署名を付加しない電子文書よりは証拠性を有しているといえるのではないかと述べ、そのような考え方に対するパネリストの見解を問うた。佐々木は、通常のデジタル署名だけを付加した電子文書を長期間利用し続ける場合、量子コンピュータの出現等、デジタル署名の安全性が「破局的」に損なわれるおそれがあるため、通常のデジタル署名を長期間利用するという考え方には問題があると指摘した。

こうした指摘を受けて、岩下は、今後デジタル署名の長期的な安全性を確保していく方法として、①通常のデジタル署名方式による署名付き電子文書の管理を第三者機関に委ね、その第三者機関の長期的な信頼性に頼るというアプローチと、②ヒステリシス署名等の特殊なデジタル署名を利用し、第三者機関には頼らないというアプローチが考えられると述べたうえで、どちらのアプローチが望ましいと考えられるかをパネリストに尋ねた。これに対し、松本は、両方のアプローチを組み合わせて個々の署名付き電子文書の安全性を高める体制を構築することが大切であると述べた。佐々木は、特定の第三者機関を現時点で信頼できたとしても、長期間継続して信頼できるとはいえないため、第三者機関に頼らなくても署名付き電子文書の安全性を長期間確保するための仕組みを検討する必要があると述べた。なお、松浦は、個々の署名付き電子文書の安全性を確保するための技術について検討する際に、

汎用的なPKIを想定した技術に関する研究なのか、あるいは、個別アプリケーションの技術に関する研究なのかを曖昧にしたまま議論されるケースが多い点を指摘し、新しい技術の効果を適切に評価するためには、その技術がどちらの範疇に属するかをきちんと意識したうえで検討を進めることが大切であると述べた。

パネリストから「個々の署名付き電子文書の安全性を確保するという視点が重要」との指摘があったことを踏まえ、岩下は、PKI等、電子認証のインフラに加えて、「デジタル署名の証拠性を長期間維持するためのインフラ」を別途構築することが必要となるのか、その場合、新たなインフラを構築するコストとベネフィットの関係をどのように考えればよいかについてパネリストに尋ねた。松本は、例えば、電子文書の証拠性を示す情報等を一定のフォーマットで電子文書に埋め込む技術が確立すれば、PKIのインフラに大きな影響を与えないで電子文書の証拠性を確保することも可能になるのではないかとの見方を示した。さらに、松本は、セキュリティの観点でPKIの枠組みに深刻な問題が発生した場合においても電子文書の証拠性を確保可能な「奥の手」となる技術が必要であることを強調したうえで、そうした技術をいかにリーズナブルなコストで実現するかが今後の重要な研究課題であると述べた。佐々木は、ヒステリシス署名等の技術が今後さまざまなアプリケーションに実装されるようになれば、そうした技術もPKIの一部として技術標準等に組み込まれるのではないかと述べた。また、松浦は、情報セキュリティ技術の費用対効果の評価に関する研究が最近いくつか発表されていることを紹介したうえで、新しいインフラの実用性や費用対効果をきちんと議論するためには、新しい技術の研究開発に加えて、情報セキュリティ技術のシステム評価に関する研究を今後推進していく必要があると述べた。

次に、岩下は、量子コンピュータの出現等によってPKI全体が突然「破局的」に脆弱化した場合の対策についてパネリストに質問した。佐々木は、現在主流となっている計算量的安全性をベースとした署名方式とは別に、情報量的安全性等、別の原理を用いた代替方式を準備しておく必要がある点を指摘したうえで、PKIの脆弱化のパターンを洗い出し、各パターンに応じてどのように署名方式の移行を実施するかを検討する必要があると述べた。松浦は、新しい技術を導入することを想定した場合、そうした技術を適切に活用することができる人材を育成しておくことも必要になると説明し、管理・運用体制の整備が重要であるとの見方を示した。松本は、現時点では鍵長1,024 bitのRSA署名方式を利用するケースが多く、当面は同方式で十分な安全性を確保できると考えられるものの、今後のコンピュータにおけるコスト・パフォーマンスの向上等を想定して代替方式を準備しておく必要があると述べた。

最後に、松本は、デジタル署名の長期的な安全性をいかに確保していくかに関する研究は非常に重要であるものの、現時点では、問題の全体像が明らかにされるまでには至っていないのが実情であり、今後も検討を続けていく必要があると指摘した。佐々木は、デジタル署名の長期的な安全性に関する研究では、現在、わが国が世界のトップクラスに位置しており、日本発の重要な基盤技術となる可能性もある

との見方を示したうえで、今後、一段と研究を深めていくことが重要であると述べた。また、松浦は、デジタル署名の長期的な安全性に関する研究を進めるうえで、開発と評価の両方の視点から検討することが重要であると述べた。

以上の自由討議を受けて、フロア参加者から、「デジタル署名の長期的な安全性を確保するために新しい技術の採用を検討しても、利用者が好んでそのような技術を利用するようになるだろうか」との質問が寄せられた。これに対して、佐々木は、デジタル署名の長期的な安全性を確保するための技術を今後研究開発していく際にも、一般ユーザーにとっての利便性に十分配慮することが重要であると述べた。また、松浦は、デジタル署名の長期的な安全性を補強する新しい技術を検討する場合には、利用者がスムーズに移行できるよう、既存のインフラを活用していくことが不可欠と述べた。

また、フロア参加者から、「現時点においてデジタル署名付き電子文書を長期間安全に保管するための最も簡便な方法は、署名付き電子文書を生成する都度必ずデジタル・タイムスタンプを生成するという方法ではないか」との指摘が寄せられた。松本は、デジタル・タイムスタンプが対応策の1つと考えられるとの認識を示しつつも、署名付き電子文書を長期間利用する場合を想定するといくつかの問題点が存在していると述べた。主な問題点として、松本は、①既存のデジタル・タイムスタンプにおいては、タイムスタンプ発行機関がデジタル署名を付与する方式が主流となっているが、そのデジタル署名の安全性が低下した場合の対応策が十分検討されていないこと、②タイムスタンプの生成に利用される日時データが改ざんされていないか否かはタイムスタンプ発行機関の信頼性に依存しており、第三者が日時データの完全性を検証する仕組みが確立していないことを挙げた。

5．総括コメント

今井は、総括コメントとして、キーノート・スピーチ、研究発表およびパネル・ディスカッションの内容を振り返ったうえで、次のようにコメントしてシンポジウムを締め括った。

今回のシンポジウムのテーマである「デジタル署名の長期的な利用とその安全性」は、デジタル署名の研究領域の中でも重要な課題の1つであるが、これまではあまり注目されてこなかった。今回のシンポジウムは、研究発表やパネル・ディスカッションにおいて中身の濃い考察・議論が行われ、関連する分野の研究者や実務家にとって意義深いものであったと思う。今後、電子文書の利用がいっそう拡大し、電子文書を長期にわたって利用することが必要となった場合に備えて、デジタル署名の証拠性を補強し、電子文書を安全に長期保管する技術を検討しておくことが必要である。今回のシンポジウムは、そうした検討を深めるための契機となったのでは

ないかと思う。

電子政府で利用される暗号技術の安全性評価については、経済産業省と総務省が主催する暗号技術検討会（CRYPTREC）において、3年間にわたる評価作業を行い、2003年2月に「電子政府推奨暗号リスト」を公表した。デジタル署名方式については、最終的に4方式（DSA、ECDSA、RSASSA-PKCS1-v1_5、RSA-PSS）がリストに掲載された。今後は、デジタル署名方式のアルゴリズムを他の技術と組み合わせた技術の評価が必要となるが、例えば、本日議論された「デジタル署名の長期的な証拠性を高める技術」も、評価対象として意識していくことが必要である。

同じく2003年2月、欧州における暗号アルゴリズム評価プロジェクトNESSIEの選考結果が発表され、共通鍵暗号方式の分野では、64 bitブロック暗号として三菱電機が開発したMISTY、128 bitブロック暗号としてNTT・三菱電機が開発したCamelliaが推奨暗号リストに含まれることとなったほか、ICカード向けデジタル署名方式として、松本・今井暗号をベースとしたSFLASHが選定された。これらの暗号アルゴリズムはいずれもわが国において研究開発された技術であり、NESSIEの選定結果は、わが国の暗号技術が世界のトップレベルにあることを証明しているといえよう。

今回のシンポジウムのテーマであったデジタル署名の長期的な安全性を確保するための技術に関しても、ヒステリシス署名や情報理論的に安全なデジタル署名方式など、わが国における研究が世界のトップを走っている。今後も、こうした研究開発をいっそう推進し、わが国から世界に向けて有用な技術が積極的に提案されることを期待したい。